09-047

11/82 (M. Levy Authorizing)

CRIMINAL COMPLAINT

United States District Court

DISTRICT: Eastern District of Pennsylvania

UNITED STATES OF AMERICA
v.
Jing HE

DOCKET NO.:

MAGISTRATE'S CASE NO.: 09-372

Complaint for violation of Title 18 United States Code § 1832

NAME OF JUDGE OR MAGISTRATE	OFFICIAL TITLE	LOCATION
Honorable Carol Sandra Moore Wells	U.S. Magistrate Judge	Philadelphia, PA

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (if known)
February 29, 2009	Malvern, PA	1504 Cardiff Terrace West Chester, PA 19038

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

Count One

On or about February 28 and 29, 2009, the defendant with intent to convert a trade secret that is related to and included in a product that is produced for and placed in interstate and foreign commerce, to the economic benefit of himself and others unknown, and knowing that the offense would injure the owner of the trade secret did steal, and without authorization by fraud, artifice and deception obtained such information.

Count Two

On or about February 28 and 29, 2009, the defendant with intent to convert a trade secret that is related to and included in a product that is produced for and placed in interstate and foreign commerce, to the economic benefit of himself and others unknown, and knowing that the offense would injure the owner of the trade secret without authorization copied, duplicated, and downloaded such information.

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

SEE AFFIDAVIT ATTACHED HERETO.

MATERIAL WITNESSES IN RELATION AGAINST THE ACCUSED:

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.

SIGNATURE OF COMPLAINANT (official title)

Denis Drum

OFFICIAL TITLE

Special Agent, Federal Bureau Investigation

Sworn to before me and subscribed in my presence.

SIGNATURE OF MAGISTRATE [1]: Carol Sandra Moore Wells

Honorable Carol Sandra Moore Wells, United States Magistrate Judge

DATE: February 27, 2009

1) See Federal Rules of Criminal Procedure rules 3 and 54.

AFFIDAVIT

I, Denis Drum, Special Agent, Federal Bureau of Investigation (FBI), being duly sworn do hereby depose and state that:

I. INTRODUCTION

1. I am employed as a Special Agent of the Federal Bureau of Investigation ("FBI"), and I have been so employed for the past seventeen years. I am currently assigned to the Philadelphia Field Office to a squad responsible for counter-intelligence matters relating to China. I have worked in the intelligence field for approximately four and a half years. In addition to my counter-intelligence assignment, during my tenure with the FBI, I have previously been assigned to conduct white collar crime investigations for ten years, including bank fraud, wire fraud and health care fraud matters. I was also assigned to international terrorism matters for three years.

2. I am currently assigned to the investigation of HE, Jing (HE). The investigation focuses on the attempted theft of trade secrets by HE from a company known to me that requests anonymity at this time, but will be further known as Company A. Company A is located in the Eastern District of Pennsylvania. I along with other agents of the FBI have been investigating HE since February 26, 2009.

3. This affidavit is submitted in support of an application for a complaint and an arrest warrant charging HE Jing with an attempt to commit a theft of trade secrets, in violation of 18 U.S.C Section 1832.

4. Information in this affidavit is based on my personal knowledge and on information provided to me by other FBI agents and analysts, and law enforcement officers, during the course of this investigation.

Background

5. HE Jing is an adult male citizen of the People's Republic of China (PRC) born on October 9, 1981. HE is a legal immigrant visitor to the United States (US). HE entered the US on a Chinese passport bearing the number

G22634414. HE entered utilizing a J-1 visa. A J-1 visa is issued to a foreign national who has been selected by a sponsor, designated by the United States Department of State, to participate in an exchange visitor program and who is seeking to enter or has entered the United States temporarily as an exchange visitor. Records indicate that HE entered the US on August 17, 2007 at O'Hare International Airport in Chicago, Illinois.

6. Company A is a multi-national corporation engaged in business worldwide.

7. HE was employed at Company A from on or about August 20, 2007 to February, 25, 2009. While employed at Company A, HE worked in a business unit of the company identified as the HSBU from August 2007 until August 2008. From August 2008 until February 25, 2009, HE worked in the IMKBU. In connection with HE's employment with Company A, HE provided information about his background. HE indicated that he had been born in Laibing, Guangxi Province, PRC. HE had come to Company A from the Department of Precision Machinery and Precision Instrumentation at the University of Science and Technology of China, 10# 222 PO Box 4, West Campus of the USTC, Hefei, Anhui, PRC 230027.

8. On Monday, February 23, 2009, HE spoke with a co-worker identified as (NK). HE asked NK where he could find source code. HE also asked the NK about the requirements for using "M", a software product of Company A. NK advised that HE had a need to know about the source code, but did not have the purpose to independently access it. HE's job duties allowed him access to the source code when assisting other individuals who were having problems with it. NK asked HE why he wanted to know. HE responded by saying he was interested in how it worked. NK added that since the week of February 23, 2009 was HE's last official week with the company, HE had no official duties. Rather, HE was handling tasks necessary to process out of the company and return to China.

9. On Tuesday, February 24, 2009, NK noticed that HE had an external computer hard drive connected to his computer laptop, a laptop issued to him by Company A. NK noticed that the hard drive was hooked up to the laptop all day. NK did not see the computer screen, nor could he say for sure that the hard drive was operating, but assumed it was based on what he observed.

10. On Wednesday, February 25, NK came to work and observed that the hard drive was still connected to the laptop. NK then asked HE what he was doing. HE responded by saying that he was copying documents to the hard drive. After the discussion with HE, NK recalled the source code discussion with HE on Monday and became suspicious. NK knew the hard drive was too large for copying documents as HE described. NK discussed his concerns with a second co-worker (CR) and his manager (NM).

11. Also on Wednesday, February 25, CR came to observe HE at his desk. CR sits diagonally across from HE. On that Wednesday, CR observed HE bring a portable computer hard drive into the office. According to CR, it was not unusual for interns like HE to have a hard drive in the office during their last week of work as they generally used it to copy personal information that had accumulated on the computer system. About an hour into the workday, CR saw an open window on the computer and could tell that HE was copying something from the computer to the hard drive. At that time, CR could not see what was being copied. Later on in the day, CR went to a meeting and returned at approximately 1:45PM. HE was still copying at that time. CR became concerned because normal copying time is approximately 30 minutes for an intern. CR arranged to get HE away from his computer so that CR and NM could see what was going on at HE's computer. According to CR, he visually verified that documents and source code were being downloaded and had been downloaded on to HE's hard drive. CR did not see anything of a personal nature of HE's being downloaded.

12. Upon HE's return to the office after the discovery by CR and the NM, HE was confronted by CR and a third co-worker (FN). HE admitted he was downloading Company A source code and VOB (folders which contain documents that among other things, provide instruction on how to manipulate the source code.)

13. After HE was confronted FN asked HE to begin deleting the downloaded material. Approximately fifteen minutes into that process, the vice-president of the business unit (MW) was contacted. MW instructed the deleting to be stopped immediately which it was. The company then seized the hard drive and the laptop from HE. HE was then brought to MW. HE acknowledged downloading the

source code, but did not say why he did it. According to MW, he was sorry and very apologetic. HE was prevented from further access to the building on that same day.

14. HE's immediate supervisor, NM advised that he spoke with HE about his actions on Wednesday, February 25th. HE was very apologetic. When NM asked why HE had done this, HE responded by indicating that he wanted a copy of the material so he could continue to learn about "ip".

15. On February 27, 2009, HE was interviewed by Special Agents of the FBI at Starbucks coffee shop at the corner of 3rd and Arch Streets in Philadelphia, PA. HE had been contacted by telephone earlier in the day and asked if he would consent to an interview with the FBI. HE agreed and drove on his own to the coffee shop. There were three FBI agents present and advised HE of their official identity by way of credentials. HE was explained the purpose of the interview. At the outset, HE was advised that the interview was voluntary and he was free to leave. HE was asked to explain what transpired at Company A during this last week. HE stated that he copied source code and other project related data from Company A's network to his personal hard drive. When asked specific files HE had copied, HE stated he copied the entire "E" project directory, the "C" directory and the "3" directory. HE estimated that he copied approximately 10 gigabytes worth of Company A data. HE was asked if he believed that Company A would allow him to take the information with him. HE acknowledged that Company A would not have allowed it.

16. During the course of the interview, one of the Special Agents contacted NK at Company A. NK was asked if the above referenced directories contained proprietary source code developed by Company A. NK confirmed that all listed directories did. NK further stated that any open source or third party tools were located in different directories.

17. Also during the interview, HE advised that he possessed two laptop computers, one hard drive and several other digital storage devices at his residence in West Chester, PA.

18. According to Company A officials, computers at the company are secured such that an individual needs a password to access the computer. Additionally, each system

available to employees has an access list which further restricts a persons access to particular areas. HE's access was based on the business unit to which he was assigned. The computer systems which HE accessed are not accessible or available to individuals outside of the company.

DENIS DRUM
Special Agent

Sworn to and
Subscribed before me
this 27th day of
February 2009

CAROL SANDRA MOORE WELLS
United States Magistrate Judge